Entrust Datacard™

+1-888-690-2424
entrust@entrust.com
entrust.com/mobile

@EntrustDatacard
+entrust
/EntrustVideo
/EntrustSecurity

Entrust IdentityGuard Mobile

Mobile Solutions for Simply Better Authentication

As mobile devices continue to expand in capability and popularity, they present tremendous opportunities for consumers and enterprises alike. This shift to more mobile-centric environments spans consumer- based activities like mobile banking or smartphone transactions, as well as more enterprise-specific tasks such as strong authentication needs for employees and privileged access users.

DOWNLOAD THIS DATA SHEET

Mobile Devices Improve Enterprise Security

Regardless of your industry, regulatory compliance and breach threats mean that you need to secure employee access to company networks and applications. While hardware tokens have been adequate in the past, the cost and management burden of this dated technology is high while your user communities continue to be frustrated, having to carry tokens and type-in lengthy one-time-passcodes when authenticating.

Entrust IdentityGuard Mobile with "push notification" makes secure access to VPNs and Web applications easier than ever – for both users and for IT support. Users simply access the VPN with their username and password, and instantly their mobile phone alerts them to verify the login using the Entrust IdentityGuard Mobile application. A quick review and click of the "OK" buttons secures the session, allowing your employees to be confident that malware has not gotten access to the network or application.

Entrust IdentityGuard Mobile supports a range of features in addition to push notification including more traditional soft-tokens, QR code scanning for easy activation where advanced transaction verification is required but mobile data connectivity is limited.

Stop Online Banking and Card Not Present (CNP) Fraud in Its Tracks

While there are many safeguards deployed inside financial institutions today, criminals are increasingly overtaking online accounts with stealthy malware and turning to new channels, such as e-commerce, which offer attractive rewards.

E-commerce fraud can be committed by simply stealing a consumer's credit card number and CVV code then making an online purchase anywhere EMV chip security is not enabled. The controls that financial institutions have put in place to combat CNP are easy to circumvent. The many ways to steal a card number creates more opportunities for fraud loss and erodes consumer confidence. To combat these attacks, Entrust IdentityGuard Mobile allows you to offer consumer digital services confidently, by engaging your customers in the fight against online fraud.

Solution Benefits

- Easy, convenient for end-users by enabling them to leverage their mobile devices
- Reduce costs and confidently migrate away from legacy hardware tokens
- Simplify IT management by empowering users with mobile-based user self-provisioning
- Strong authentication with patent pending out of band transaction verification to defeat advanced session riding attacks
- Flexibility to support users without mobile offering the broadest range of authenticators on a single platform including: mobile authenticators, physical or electronic grid cards, KBA, adaptive authentication, and even hardware tokens for those who don't like change
- Migrate with ease – with Entrust you can co-deploy alongside a legacy solutions such as RSA and migrate users as hardware tokens expire.

Three Authentication Tools for Financial Institutions

Mobile One-Time-Passcode Tokens

Entrust enables organizations to transform smartphones into convenient, secure one-time-passcode (OTP) tokens, leveraging devices that are widely deployed, to provide convenient security for online banking. Organizations can also brand these soft tokens for better customer or employee recognition.

Out-of-Band Verification

Entrust's mobile application provides out-of-band notification of transaction details to enable users to confirm the legitimacy of transactions or immediately report fraud by simply declining the transaction. Entrust IdentityGuard also includes the ability to store and refer to transaction history. Options for online push notifications and offline QR code scanning provide organizations with the flexibility they need to meet varied user communities, such as those without a data plan. This is a proven method that helps defend against today's advanced malware, like man-in-the-browser attacks.

Transparent Strong Authentication

Entrust's easy-to-use software development kit (SDK) helps organizations embed transparent strong authentication right into their own mobile application. This provides transparent security for consumers using mobile banking, while enabling organizations to enhance security for the online channel.

And embedding OTP technology in a mobile device is more cost-effective than purchasing, issuing and deploying hardware tokens because it leverages devices that are already widely deployed — increasing user acceptance.

Product Benefits

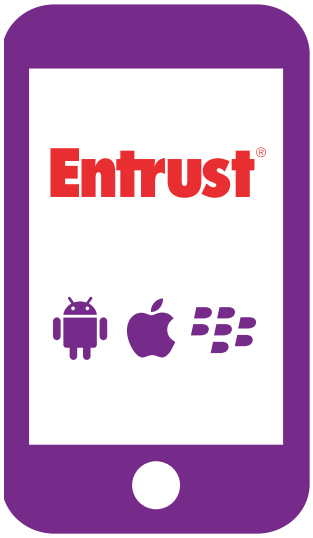
- Enables strong mobile authentication with out-of-band transaction confirmation
- Leverages mobile devices to boost authentication strength without inconvenience
- Provides two-factor authentication for customer or enterprise environments
- Transforms today's popular smartphones into mobile credentials
- Includes standards-based (OATH) authentication and signature
- Support for leading mobile platforms including Apple iOS, RIM BlackBerry, Google Android, and Microsoft Windows Mobile
- Customizable to include organization-specific branding for increased user acceptance

Stronger Authentication via Mobile Devices

Entrust provides trusted identity and authentication in distinct solution areas — mobile authentication, online web authentication, and transaction verification to defeat account takeover and card-not-present fraud.

While supporting a broad range of use cases brings many benefits, Entrust IdentityGuard Mobile is also extremely secure with a range of layered security controls including protection against any compromise of the mobile operating system by storing mobile identities within the Trusted Execution Environment (see page 4).

ENTRUST MOBILE SECURITY SOLUTIONS
IDENTITIES, DEVICES & TRANSACTIONS



STRONG AUTHENTICATION

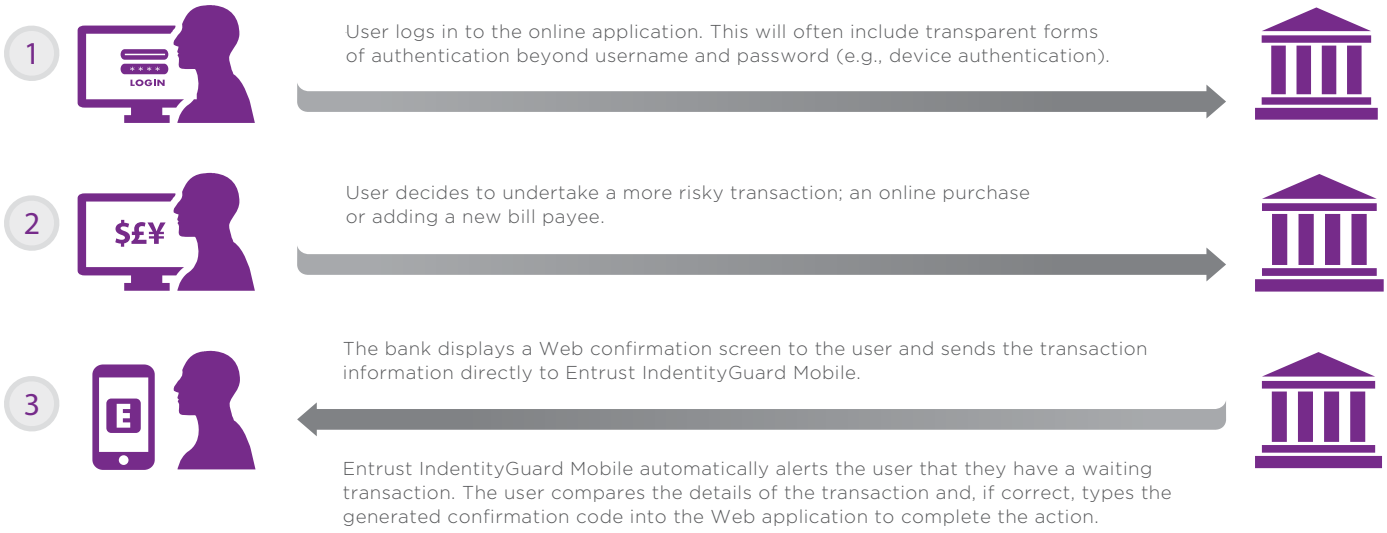
TRANSACTION VERIFICATION

CNP FRAUD

ADAPTIVE AUTHENTICATION

SECURE IDENTITIES WITH TEE PROTECTION

Entrust IdentityGuard Transaction Verification - How it Works



A common example of how Entrust IdentityGuard Mobile helps authenticate and verify a Web-based transaction via a mobile device.

Advantages

Convenient Mobile Push Authentication.

Transform smartphones into convenient, secure OTP based authenticators for employees and customer alike. Along with eliminating the need to provision and carry hardware tokens, our push notification approach dramatically simplifies the user experience and eliminates the need to type in OTP values during login. This approach has a high user-adoption rate and can include organizations-specific branding for better customer or employee recognition.

Defeat Account Takeover and CNP fraud

Entrust IdentityGuard Mobile transaction verification is a consumer friendly solution that can be used to defeat advanced malware, and account takeover attacks such as man-in-the-browser (MITB) attacks. In addition, the same solution can be used to prevent CNP fraud in real time, providing the perfect security compliment to EMV card security.

Reduce IT Cost and Complexity

Leveraging mobile eliminates the need to purchase dedicated hardware authenticators and simplifies user provisioning and management as users already know how to download and update mobile apps and Entrust's broad range of self service features makes enrollment and activation a breeze.

Easy Integration

Entrust's open API architecture allows for tight integration with today's leading mobile device management (MDM), identity access management (IAM) and public key infrastructure (PKI) vendors. This enables Entrust IdentityGuard to work with new and existing enterprise implementations, plus adds the ability to integrate in-house or managed service-based digital certificates.

Broad Platform Support

Supports the leading mobile platforms on the market today, including Apple iOS, RIM BlackBerry, Google Android, and Microsoft Windows Mobile.

Customizable

Includes the ability to add organization-specific branding to each identity, improving usability and reinforcing brand image.

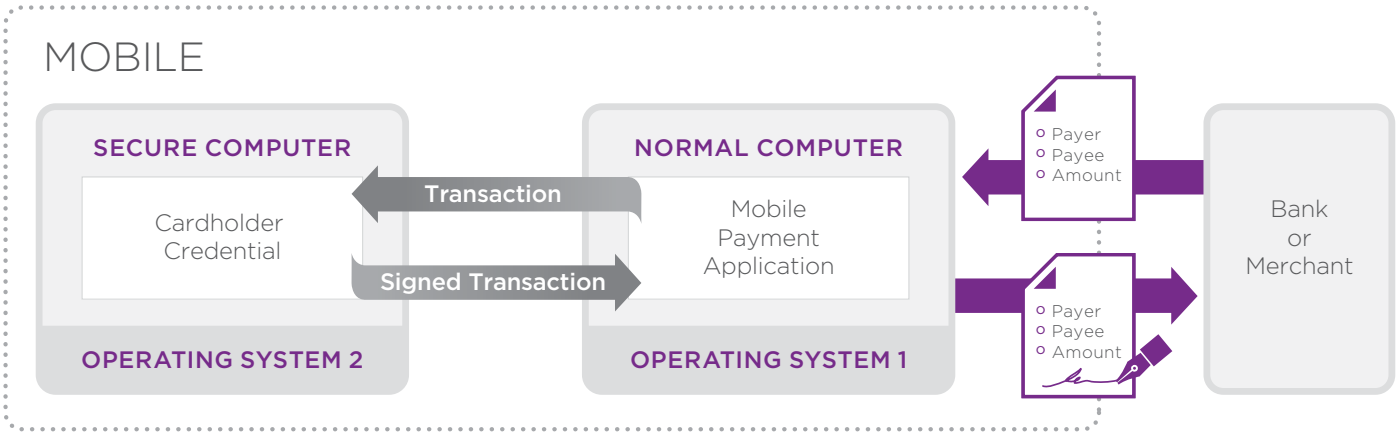
For Developers

Entrust's easy-to-use SDK helps organizations embed transparent and strong authentication right into their own mobile applications.

Entrust IdentityGuard Mobile

Mobile Solutions for Simply Better Authentication

The Security of the Chip Credit Card, the Convenience of a Mobile Application



The Entrust IdentityGuard Mobile Soft Token Solution has the security of an EMV chip credit card, but the convenience of a mobile application. This is made possible through:

- Storing the credential in the Trusted Execution Environment (TEE), the hardware protection available in modern mobile devices. The TEE essentially allows for a second computer within the mobile device, which can be dedicated to your digital identity. Any defect in the operating system does not allow for the credential to be stolen or misused. It is like sending the transaction to your card for approval.
- Recording the fingerprint of the device itself when the credential is issued. This keeps the credential from being stolen and moved onto another device when hardware protection is not available.
- Replacing the PIN with a fingerprint. No number to remember, prevents unauthorized use, while being easy to use.
- Comprehensive Adaptive Authentication to only involve the consumer when the risk is high.

The convenient, strong authentication allows for services not previously possible:

- Financial transactions or purchases are sent to the consumer's device for instant approvals, preventing unknown fraudulent purchases made against your account number.
- Digital signatures of loan applications, eliminating the need to travel to the bank branch.

About Entrust Datacard
Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Entrust Datacard™

30112-1-0216